Semiconductors

UM

DESFireUI; Demo software for DESFire and DESFireSAM

Rev. 01 — 27 May 2005 **User manual**

Document information

Info	Content
Keywords	DESFire, DESFireUI, DESFireSAM, SAM, AID, 3DES, demo software
Abstract	This document describes how to use the DESFireUI demo program to experience the functionality of the DESFire, the DESFireSAM and both products combined. DESFireUI communicates with the DESFire through an RD700 or RD701 reader and with the DESFireSAM through a contact smartcard reader with a PC/SC interface.
BL-ID Doc Number	M111010

PHILIPS

Revision history

Rev	Date	Description
01	20050527	Initial version of the DESFireUI User Manual

Contact information

For additional information, please visit: **http://www.semiconductors.philips.com**

For sales office addresses, please send an email to: **sales.addresses@www.semiconductors.philips.com**

1. Introduction

DESFireUI is a demonstration program that can show the functionality of the DESFire smartcard (see Ref. [1]) and both versions of the DESFireSAM; the full version (see Ref. [3]) and the DESFireSAM MAC, the restricted version that has the feature to encrypt data disabled (see Ref. [4]).

The core of the program consists of two parts; one part for the DESFire and a second part for the DESFireSAM. Both parts can be used independently of each other, but the DESFireSAM part can be used to load keys used by the DESFire part. For example, new keys can be downloaded manually to the DESFire, but with an activated DESFireSAM the manual key-loading is disabled and DESFireUI only allows downloading the keys through the DESFireSAM.

The first part of the demo program allows the user to execute all DESFire commands, and learn more about the functionality of the DESFire. It communicates with a DESFire through the contactless interface of an RD700 or RD701 reader (some times also called Pegoda reader).

The second part of the demo program allows the user to execute the majority of the DESFireSAM commands and learn more about the functionality of the DESFireSAM. This part communicates with DESFireSAM through a contact smartcard-reader with a PC/SC interface.

Since the main purpose of the demo program is to assist the user in gaining practical experience, it also allows malfunctions in the logical flow of commands to happen. Therefore it is possible to completely destroy the content of a DESFire. E.g. keys could be exchanged by accident and if the user does not know the value of the new key the card might be destroyed.

DESFireUI runs on Windows ME, Windows 2000 and Windows XP. On Windows NT 4.0 the reader devices attached to the USB port are not supported.

Remark: DESFire SAM functionality is only supported Windows 2000 Professional and by Windows XP.

1.1 Summary of the document content

Section 2 provides a general explanation of the DESFireUI user interface.

Section 3 provides the description on how to use all commands to interact with the DESFire Smart Card.

Section 4 provides the description on how to use commands to interact with the DESFireSAM.

Section 7 contains a reference to the datasheets of the products and an application not with features and hints that contains detailed information how the DESFire can and should be used. Their content is essential to understand the examples in the back of the document.

Section 5 provides some samples of command sequences on how to execute some basic functions of the DESFire, the DESFireSAM and how they can work together.

Remark: This document assumes that the user is familiar with the ISO14443 specification for contactless communication.

2. Operating instructions

The DESFireUI software can be downloaded in a ZIP-file from Philips Semiconductor's Identification website. After extracting all files the program can be started by double clicking the file **DesfireUI.exe**. A dialog window appears that is divided into several sections:

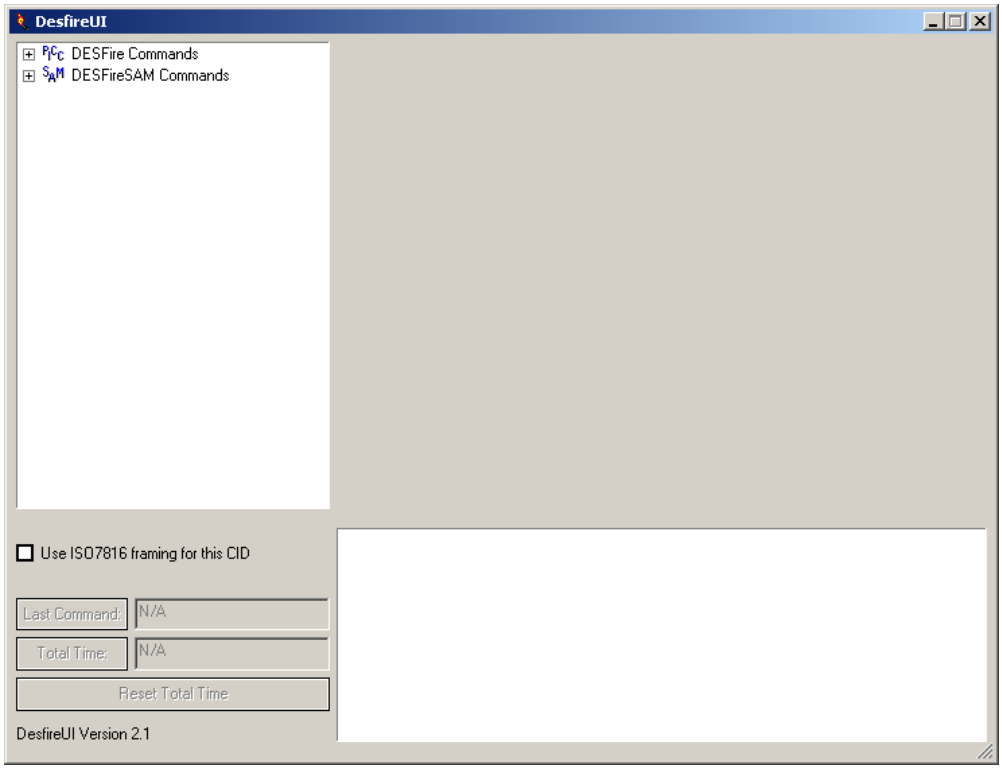

Fig 1. DESFireUI dialog window

The upper-left section shows all commands that can be send to the DESFire and DESFireSAM. Clicking the "+" signs opens up several command sections and after clicking all "+" signs it shows all available commands.

The upper-right section contains the dialog section for all commands. It will show all parameters and command boxes for the selected command.

The lower-left section contains some tools to measure command execution times for the DESFire operation.

The lower-right section contains the transaction log window. Scroll bars will pop-up as soon as the content of the window extends the space on the screen.

3. DESFire commands

3.1 DESFire command dialog window

The DESFire commands become visible as a tree after a mouse click on the “+” sign. Further clicking on the “+” signs will reveal all commands per section. Clicking on a command name will select it and the corresponding command dialog window will open up in the upper-right section:

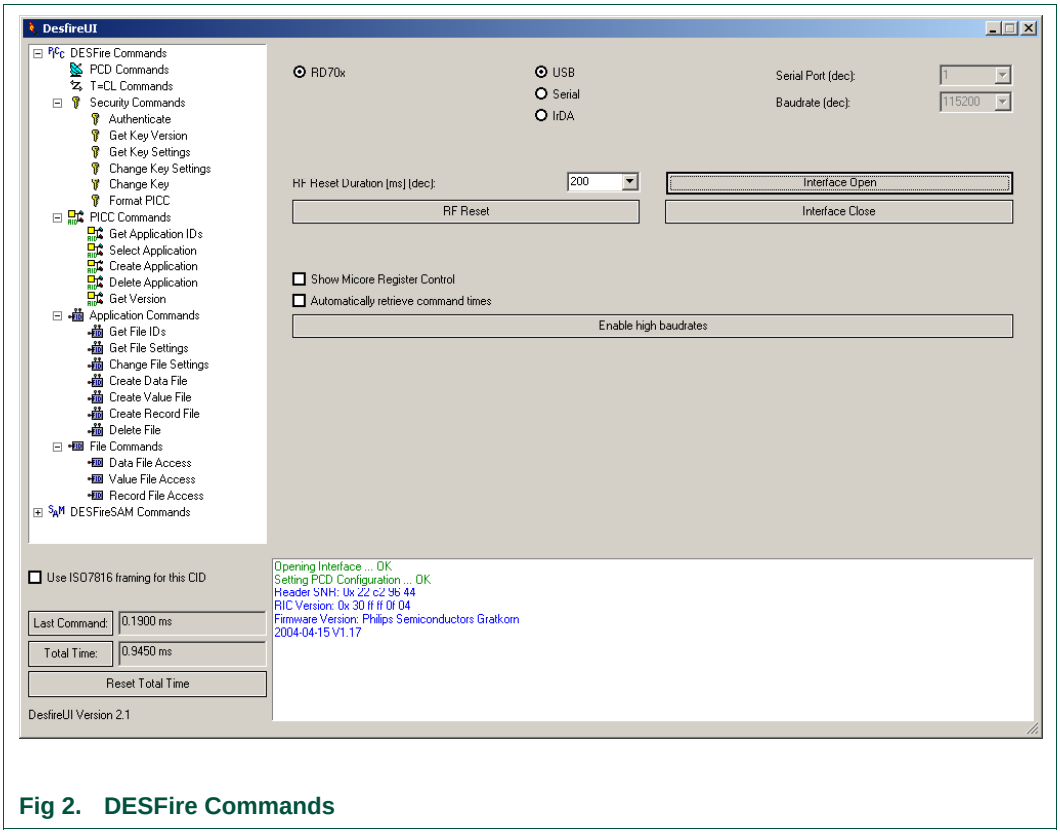

Fig 2. DESFire Commands

3.2 PCD Commands

DESFireUI only supports the RD700 and RD701 reader.

By default DESFire uses the USB interface. It also supports the version with an RS232 interface. Selecting the RS232 button enables the setting of the RS232 interface parameters **Serial Port** and **Baudrate**[1]**.**

3.2.1 Interface Open

Before any command can be send the interface with the reader needs to be opened by clicking the **<Interface Open>** box. Correct execution of the command is shown in the **transaction log** window, where also some additional information about the reader will be presented.

3.2.2 Interface Close

Clicking the **<Interface Close>** box closes the interface that was previously opened with the **<Interface Open>** box.

1. The **IrDA** checkbox is only supported for internal Philips test purposes.

3.2.3 RF Reset

An RF Reset can be used to reset any card in the RF field of the reader, equal to power cycling the cards or more simply stated, “equal to removing the cards from the field”. The duration of the reset time can be entered in the **RF Reset Duration** field.

Clicking the **<RF Reset>** box causes a reset of the RF-field of the reader (turns it off or on). The result is shown in the transaction log window.

Possible reset values range from 0 up to 255 milliseconds. The value zero has a special function and turns off the RF field permanently. To turn the RF field on again another RF Reset command is required with a value different than zero.

3.2.4 Options available for RD70x

Opening the RD70x interface successfully enables boxes for additional commands.

3.2.4.1 Show Micore Register Control

Checking the **Show Mifare Register Control** box causes the **Micore Register Control** window to pop-up, enabling the user to view and modify the values of the internal registers of the Micore reader IC in the RD70x reader[2].

Warning: The unwanted change of registers can cause damage of the RD70x!

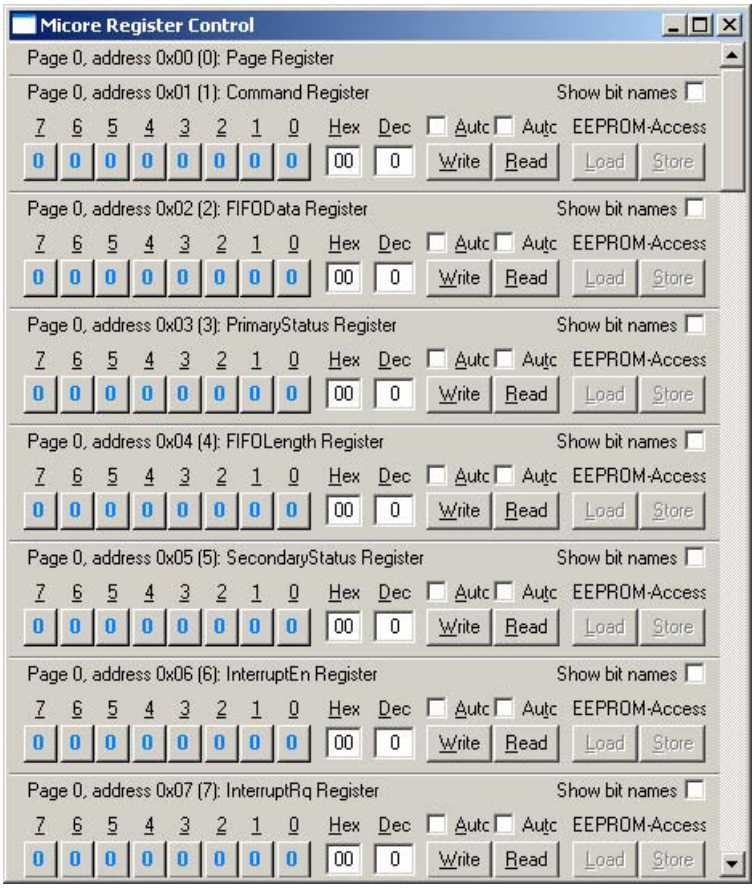

Fig 3. Micore Register Control

2. For more information about the registers please see the datasheets of the Micore reader ICs.

3.2.4.2 Enable High Baud rates

The RD701 contains the RC632 Micore reader IC that can support baud-rates up to 424 kbit/s from the PCD to the PICC and up to 848 kbit/s from the PICC to the PCD. By default the RD701 behaves only supports 106 kbit/s. However the firmware is prepared to also support the ISO14443 higher baud rates. Clicking the **<Enable high baud rates>** box enables communication with higher Baud rates.

The baud rates between the PCD and PICC can be set with the **<PPS box>** in the T=CL commands (see Section 3.3.4).

Remark: This allows the user to perform time measurements on the DESFire commands, also with different baud rates.

3.2.4.3 Automatic retrieval of command execution times

The RD70x contains two distinct timers that can measure the communication time of the most recent RF communication and also monitor the incremental time of all RF communication since the last timer reset.

Clicking the **<Automatically retrieve command times>** box enables DESFireUI to automatically retrieve the command execution time from the RD70x reader every 500 ms.

The lower-left section of the DESFireUI window contains some controls for time measurements. The **<Last Command>** box and **<Total Time>** box enable the user to measure the execution time per command and the incremental time for all commands respectively. The times are displayed in the two text display fields next to the boxes. The **<Reset Total Time>** box resets the incremental time in the RD70x.

3.2.5 Selecting the DESFire APDU format

The checkbox **Use ISO7816 framing for this CID** allows the user to let the DESFireUI communicate in either the native DESFire format or the ISO7816 APDU format.

This allows the user to experience the differences in command execution time in either the proprietary format or the ISO7816 APDU format[3].

3.3 T=CL Commands

T=CL refers to a standardized protocol (as described in ISO14443 part 4) developed to support the exchange of commands in a contactless environment.

According to ISO14443 the PICC activation process starts with some lower level ISO14443 commands and then moves to the ISO14443 part 4 level.

Therefore this section contains all commands to activate a PICC and enable communication on ISO14443 part 4 level.

The available commands are sorted in logical ISO14443 order.

3.3.1 Leave Test OS

This command is only available for Philips internal evaluation purposes and is not supported for ordinary use.

3.3.2 Activate Wakeup, Activate Idle and Halt

These commands reflect the initial states of a PICC as described in the state diagrams of the ISO14443 specification.

3. Although the DESFire does not allow switching between these two formats during an active session, it is possible within DESFireUI to demonstrate the failure effect.

- The **<Activate Idle>** box represents the ISO/IEC 14443 commands REQA, Anticollision and Select (anticollision loop incl. all cascade levels).
- The **<Activate Wakup>** box represents the ISO/IEC 14443 commands WUPA and Select (incl. all cascade levels).
- The **<Halt>** box represents the ISO/IEC 14443 command HALTA.

To activate a PICC after entering an RF field it needs to go through a sequence of commands. Initially it can be activated with the **<Activate Idle>** box. According to ISO14443 it can then be selected and de-activated (put to sleep) with the **<Halt>** box. A de-activated card can be activated again with the **<Activate Wakeup>** box[4].

Remark: These boxes execute all the detailed operations as specified in the ISO14443 specification to activate a card. Please see those specifications for more information.

3.3.3 RATS and Deselect

To establish a T=CL connection with a DESFire the **Request for Answer To Select** (also called RATS) needs to be sent to the PICC. RATS could convey the **Card IDentifier** (or CID), which uniquely identifies the PICC according to ISO14443 part 4.

The CID can be set in the **CID** field to the right of the **<RATS>** box. Possible values range from 0 to 14, where the zero has the special meaning of ***No CID***. Activating the PICC with CID zero prevents the activation of more cards using different CIDs.

After a successful reception of the **Answer to Select** (or ATS), the card is enabled for T=CL communication. If more than one CID is assigned, this means more than one card is active in the RF field and able to communicate with the PCD. In that case the value of the CID box is used to address an APDU for a specific PICC.

This allows communication with more than one DESFire at the same time.

Clicking the **<Deselect>** box deactivates a card and put it to sleep. To reactivate a deselected card it is necessary to click both the **<Activate Wakeup>** and also the **<RATS>** box again.

3.3.4 Protocol and Parameter Selection

ISO14443 specifies PPS as a special APDU to change communication parameters (like the baud rate) to values different from the default. The default **Send and Receive Dividers** are zero, referring to 106 kbit/s. If both the PCD and the PICC are supporting higher communication speeds the PPS command can be used to select different dividers (and thus different baud rates).

The dividers can be selected in the text fields to the right of the **<PPS>** box. DSI is the divider for communication from the PICC to the PCD; DRI refers to the communication from the PCD to the PICC. Possible values can be 0, 1, 2 or 3, reflecting the baud rates 106, 212, 424 and 848 kbit/s.

Clicking the **<PPS>** will set the communication settings for the RF communication.

The PPS command can only be sent immediately after a RATS command.

Remark: The RD700 only supports 106 kbit/s and the execution of a PPS command with a higher baud rate will result in an error. The RD701 supports higher baud rates, but after opening the interface they need to be enabled with the **<EnableHighBaud rates>** box. Please see Section 3.2.4.2 for more information.

4. When a card is removed from the field before it is formally “deactivated”, the DESFireUI will not allow execution of the RATS command again and will show an error message in the transaction log window. A Deselect command needs to be send before the PICC can be activated again

3.4 Security Commands

The **Security Commands** group contains the security related commands of the DESFire.

3.4.1 Authenticate

Performs the Authentication with the selected Application ID using the Key Number and Key that can be selected from or entered in the **Key Number** and **Key** fields.

Valid range for the key number is zero to 14. The key has a length of 16 bytes that are entered as 32 hexadecimal numbers[5].

Clicking the **<Authenticate>** box perform the authentication with the currently selected Application ID.

The result of the operation is shown in the transaction log window.

3.4.2 Get Key Version

Clicking the **<Get Key Version>** box retrieves the version of the specified key from the PICC and displays it in the transaction log window.

3.4.3 Get Key Settings

Clicking the **<Get Key Settings>** box retrieves the settings for the specified key and displays them by setting or clearing the corresponding checkboxes and the **Access Rights** field.

3.4.4 Change Key Settings

Utilizes the same controls as the **Get Key Settings** command, but this time it is possible to modify the settings.

Clicking the **<Change Key Settings>** box will modify the settings according to the value of the corresponding checkboxes and the **Access Rights** field.

3.4.5 Change Key

Allows changing the value of a selected key. The number can be entered or selected in the **Key Number** field. The new value for the key can be entered as 32 hexadecimal digits or selected from a previous value in the **Key** field.

Depending on the access rights it might be required to not provide the value of the previous key. In that case the **Prev. Key** field must be left empty (that means also without spaces).

Clicking the **<Change Key>** box will replace the value of the selected key.

3.4.6 Format PICC

Formatting the DESFire deletes any application permanently from the PICC, including all data files. The format PICC operation **will not** change the value of the master key. To execute the **Format** command it is necessary to first select AID zero and successfully perform an authentication with the master key.

Unlike the **Delete File** and **Delete Application** commands this also frees the memory that can then be re-used.

Clicking the **<Format Picc>** box will format the DESFire and release all EEPROM space.

5. The DESFire leaves the production facility without any user data structure and just key zero as the masterkey for the card containing all zeroes.

3.5 PICC Commands

These commands can only be executed if AID zero is selected.

The **<Get Version>** command is an exception to this rule and can be send at any time.

3.5.1 Get Application IDs

Clicking the **<Get App Ids>** box retrieves the list of available AIDs from the PICC and populates the **Application ID** field on the top of the dialog window. This selection box can later be used to select one AID from the AIDs that are available on the PICC (i.e. for the **Select Application** command).

3.5.2 Select Application

Clicking the **<Select App>** box selects the indicated Application ID. The requested AID can manually be entered or selected from the **Application ID** field.

To automatically fill the drop down box with available AIDs issue a **Get Application IDs** command (see Section 3.5.1) first.

3.5.3 Create Application

This command allows creating a new application on the DESFire. The new AID must be unique to the DESFire. Every AID needs at least one key and can have maximum 14 keys. The access conditions for the application need to be specified in the selection boxes. It also requires a key number to change the access conditions and values of the other keys in the application[6].

Clicking the **<Create App>** box creates the Application ID on the PICC.

3.5.4 Delete Application

Clicking the **<Delete App>** box deletes the application indicated by the **Application ID** field.

Remark: The memory space that becomes free because of this deletion cannot be used again for another file. Only the Format DESFire command can empty the PICC and make all memory available again.

6. Entering the value 1 to 9 will result in the AIDs 10h to 90h.
To enter AID 1 you need to enter the value 01h

3.5.5 Get Version

Clicking the **<Get Version>** box retrieves manufacturing information from the DESFire and shows it in the transaction log window.

Table 1: DESFire Get Version information

Hardware info	Software info part 1	Software info part 2
• Vendor ID: (0x04 for PHILIPS) • Type • Sub Type • Major Version • Minor Version • Storage Size: • Protocol	• Vendor ID: (0x04 for PHILIPS) • Type • Sub Type • Major Version • Minor Version • Software Storage Size: • Protocol - 0x05 for ISO 14443-2 and -3	• UID: 7-byte UID • BatchNo batch number • Production CW calendar week of production • Production Year year of production

3.6 Application Commands

The **Application Commands** can be used to perform file management. They can only operate on AIDs other than zero.

Remark: Authentication using the appropriate access rights (configured when the application was created using Create Application command; see Section 3.5.3) will be required if the application has not been set up to allow free use of the applicable functions described in this section. An error code (Error code: 1be, Unknown error) will be returned if this not done.

3.6.1 Get File IDs

Clicking the **<Get File ID>** box retrieves all File IDs (FIDs) that exist within the selected AID and shows them in the transaction log window.

This command also populates the **File ID** selection box with available FIDs. This box can then be used to select an FID later.

3.6.2 Get File Settings

Clicking the **<Get File Settings>** box retrieves the settings for the selected **File Id**. The information is shown in the controls for the encryption mode and various access rights and in the transaction log window.

Some more information like the file type and size is shown in the log window.

3.6.3 Change File Settings

This command uses the same interface as the **Get File Settings** command (Section 3.6.2), but now the encryption mode and access rights for the specified FID can also be changed. Clicking the **<Change File Settings>** box changes the settings for the selected **File Id**.

3.6.4 Create Data File

This command can be used to create a custom data file and provides options to select the encryption mode for data communication with the PCD and the access rights.

The required size of the file (in bytes) can be entered in the **File Size** field. Checking the **Backup File** option enables the on-chip backup mechanism for the file, but that also doubles the required memory space for this file. The file size and the backup option determine the EEPROM space that will be occupied. These values cannot be modified after the file has been created.

Clicking the **<Create Data File>** creates the file within the selected AID.

3.6.5 Create Value File

This command can be used to create a value file and provides options to select the encryption mode for data communication with the PCD and the access rights.

A value file requires a setting for the **Upper Limit**, the **Lower Limit** and for the **Initial Value**. These values can be entered in the corresponding fields.

Checking the **Limited Value** box enables the limited value option.

Clicking the **<Create Value File>** creates the file within the selected AID.

Remark: Value files always use DESFire's backup feature and require double the memory of the anticipated for value data used.

3.6.6 Create Record File

This command can be used to create a record file and provides options to select the encryption mode for data communication with the PCD and the access rights.

A record file requires a setting for the **Record Size** and the **Number of Records**. These values can be entered in the corresponding fields.

Checking the **Cyclic File** box turns the file into a Cyclic File (in stead of a Linear File).

Clicking the **<Create Record File>** box creates the file within the selected AID.

Remark: Record files always use DESFire's backup feature and require double the memory of the anticipated for record data used.

3.6.7 Delete File

Clicking the **<Delete File>** box deletes the file within the selected AID.

The memory space that becomes free because of this deletion cannot be used again for another file[7].

3.7 File Commands

The **File Commands** can be used to exchange data between PCD and PICC. The commands are divided into three subcategories, one for each of the available file types. They can only operate on AIDs other than zero.

Any operation requires the selection of an existing FID. A list of valid FIDs can automatically be obtained by issuing the **Get File IDs** command from the **Application Commands** group (Section 3.6.1)

Remark: Authentication using the appropriate access rights (configured when the file was created using Create File commands in the Application Commands) will be required if the file has not been set up with free use of the applicable functions described in this section. An error code (Error code: 1be, Unknown error) will be returned if this not done.

7. Only the Format DESFire command can empty the PICC and make all memory available again.

3.7.1 Data File Access

Allows reading data from and writing data to the file with the selected FID. Clicking the **<Read Data>** box will read the data from the file, starting from the given **Offset** and up to the **Length** specified. The data being read is shown in the **Data** field. Specifying a length of zero bytes reads the entire file.

Data to be written into the PICC can be entered as hexadecimal digits into the **Data** field. When the data is entered, the program automatically counts the number of bytes in the **Length** field. Clicking the **<Write Data>** box writes the data to the file, starting from the given **Offset**.

3.7.2 Value File Access

The file is selected by the value in the **File Id** field.

Clicking the **<Get Value>** box reads the value from the file and displays the value in the **Value** field.

Clicking the **<Credit>** box adds the value of the **Value** field to the content of the file.

Clicking the **<Limited Credit>** box adds the value of the **Value** field to the content of the file, with a maximum of the limited credit value that is stored on the PICC[8].

Clicking the **<Debit>** box subtracts the value of the **Value** field from the content of the file.

Remark: Since the value file is a backup file, any modification to the value requires clicking the **<Commit Transaction>** box to actually execute the command.

3.7.3 Record File Access

This command allows to read from, write to and clear records from the file selected by the **File ID** field. Only records that are written can be read. (The record file is not a table with empty records. The records are created when the data is written). If more than one record is written, a record can be read selectively by specifying the **Start Record** and the **Number of Records**. The latest record written is selected by entering zero for the start record. The maximum number of records that can be read from a cyclic record file is always one less than the full number of records configured for that file.

Clicking the **<Read Records>** box reads **Number of Records** records from the file, beginning by **Start Record**. The content of the records is shown in the transaction log window.

Clicking the **<Write Record>** box write the content of the **Data** field to a new record, starting at **Offset**. The sum of length of the content in the Data field and the offset must be smaller than the record length.

Clicking the **<Clear Records>** box deletes all records from the record file.

Remark: Any modification to a Backup file requires clicking the **<Commit Transaction>** box to actually execute the command. All file operations performed since the last Commit Transaction command can be discarded by clicking the **<Abort Transaction>** box, thus restoring the original value

8. The value of limited credit that is stored in the PICC can be read with the Get Key Settings command

4. DESFireSAM commands

4.1 DESFireSAM command dialog window

The DESFireSAM commands become visible as a tree after a mouse click on the “+” sign. Further clicking on the “+” signs reveals all commands per section. Clicking on a command selects it and opens up the corresponding dialog in the upper-right window:

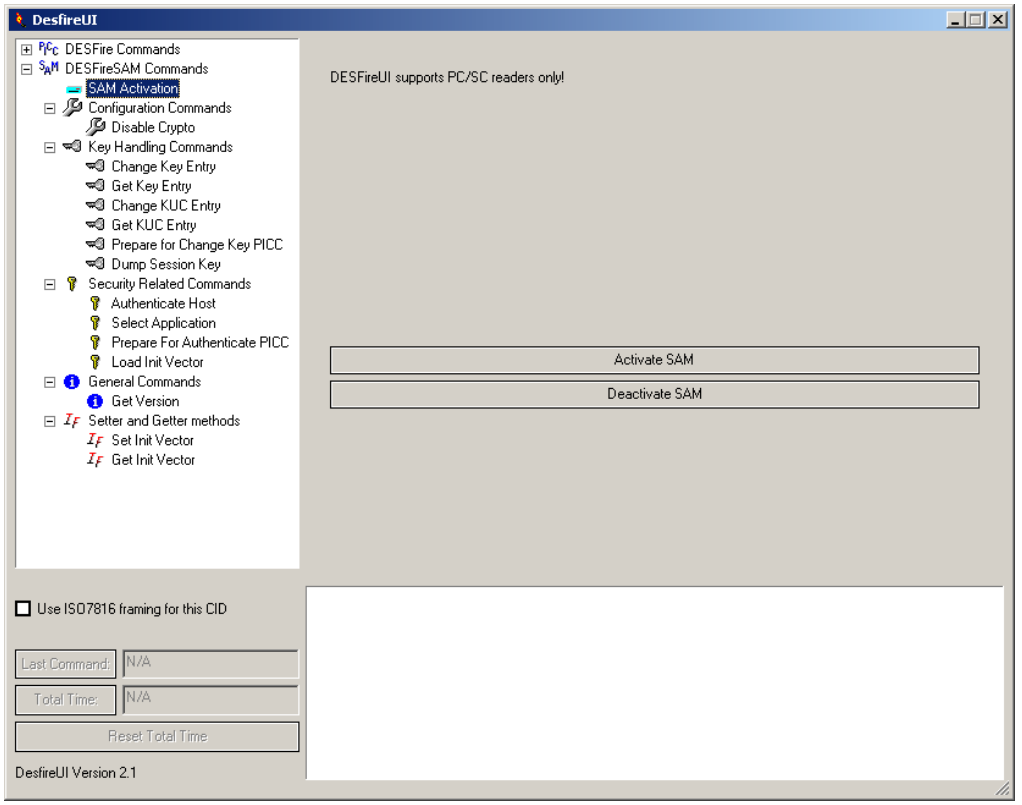

Fig 4. DESFireSAM Commands

4.2 SAM Activation

For the DESFireSAM the DESFireUI only supports smartcard readers with a PC/SC interface.

Clicking the **<Activate SAM>** box initiates a search for a PC/SC reader with a DESFireSAM present. Available options will be presented and the user can select the reader that should be used. The SAM in the selected reader will be activated and the result will be shown in the transaction log window.

4.3 Configuration Commands

4.3.1 Disable Crypto

This command allows disabling the cryptographic functionality of the SAM permanently and irreversibly.

The command provides check boxes for:

- Disable Change Key PICC
- Disable Decryption
- Disable Encryption
- Disable Verify MAC
- Disable Generate MAC

Remark: Successful host authentication with the one of the three key versions stored in KeyNo 00h is required before this command can be executed.

4.4 Key Handling Commands

The **Key Handling Commands** group contains all commands to handle the keys and related parameters. Most commands require authentication with the host before they can be executed. Exceptions to this rule are:

- Get Version
- Get Key Entry
- Get KUC Entry

4.4.1 Change Key Entry

This command can be used to update any key entry stored in the DESFire SAM.

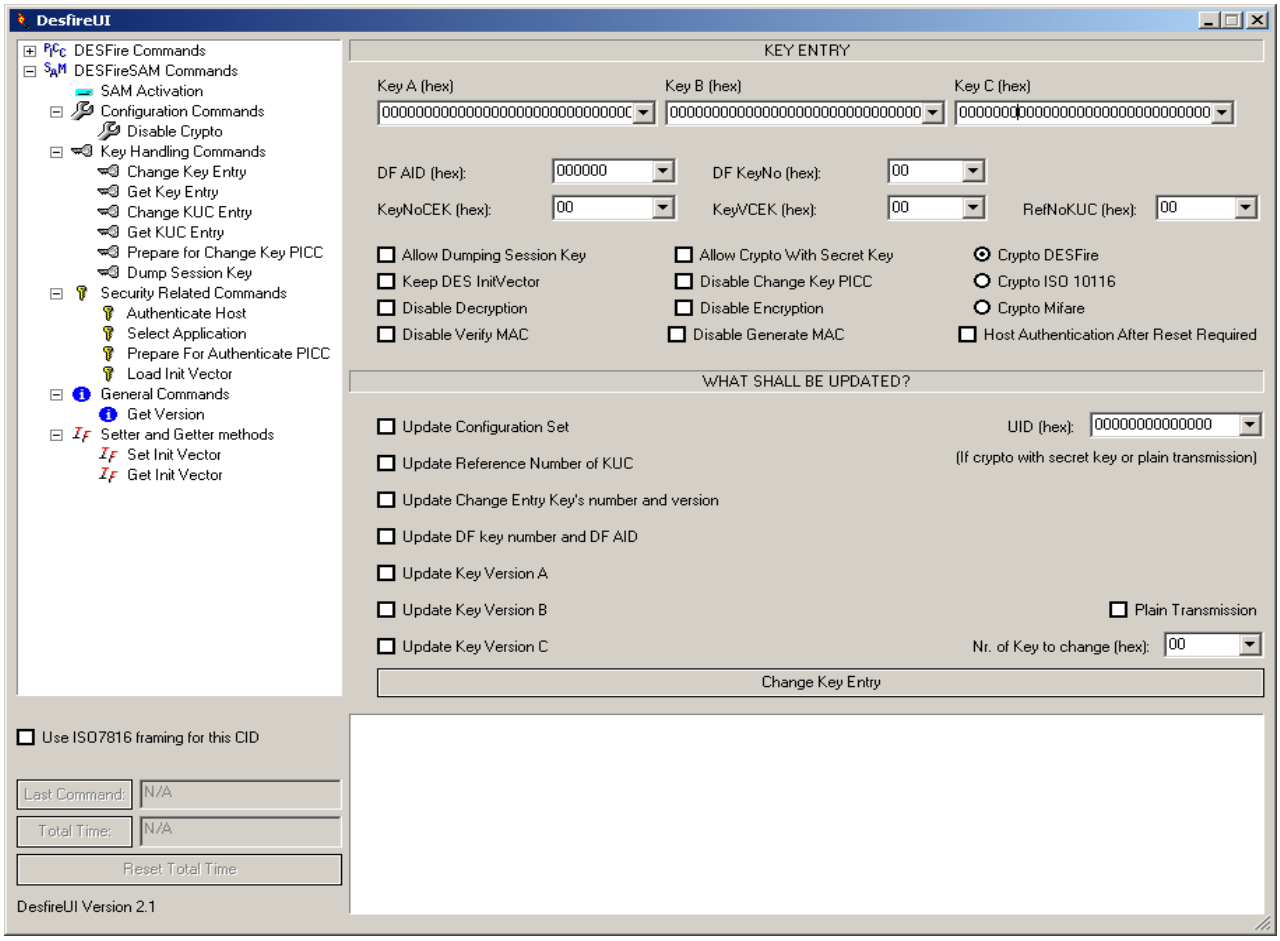

Fig 5. Change Key Entry dialog window

The command provides option boxes to enter new keys for key version A, B and C.

For communication with the DESFire there is also an entry field for the DESFire AID and DESFire key number.

Every key entry is linked to a Change Entry Key (CEK) and a Change Entry Key version. The command provides a field to enter the data.

The last entry field is for the Key Usage Counter (KUC) that counts the number of times this key has been used. The (default) value FFh for the KUC indicates that no KUC will be used.

4.4.1.1 Configuration Setting for Key Entry

The Change Key Entry command also allows changing the configuration settings of a key entry and provides check boxes for:

- Allow Dumping Session Key
- Allow Crypto With Secret Key
- Keep DES InitVector
- Disable Change Key PICC

- Disable Decryption
- Disable Encryption
- Disable Verify MAC
- Disable Generate MAC
- Enable Host Authentication after Reset (only valid for **KeyNo** 00h)

In the default configuration all DES / 3DES operations will be completed as defined in the DESFire MF3ICD40 datasheet (Ref. [1]). However by selecting the corresponding checkbox the DES / 3DES can also be performed as defined in ISO/IEC 10116:1997, chapter 6.

In the future a key entry can also be used to generate diversified mifare standard keys. [9]

Host and PICC authentication with this DES / 3DES key will NO longer be possible if configured for mifare key diversification.

4.4.1.2 Update Setting for Key Entry

The Change Key Entry command allows selective programming of the key entry. It provides check boxes to change:

- Update Configuration Set
- Update Reference number of KUC
- Update Change Entry Key's number and version
- Update DF Key number and DF AID
- Update KeyVa
- Update KeyVb
- Update KeyVc
- Nr of Key Entry to change

If **Crypto with Secret key** is configured for the **KeyNoCEK** AND the session key is a secret key (not based on random number), then the 7 byte UID of the DESFireSAM has to be appended to the new key before encryption to assign this command message to a specific DESFire SAM. This will dedicate the generated cryptogram to the unique DESFire SAM and will not work with another SAM. The command provides an entry box to enter the UID of the SAM. This box is automatically populated with the Get Version command; see Section 4.6.1.

If KeyNoCEK is set to FEh, the key entry is transmitted in plain, but still a 2 byte CRC and padding with 00h has to be applied. The **Plain Transmission** checkbox can be used to transmit the entry in plain text.

Clicking the **<Change Entry Key>** box actually changes the configuration and contents of the key entry according to the selections in the dialog window.

Remark: Successful host authentication with the key specified in KeyNoCEK of the selected key entry to change is required.

4.4.2 Get Key Entry

The Get Key Entry command allows reading data from the key entry specified in the **Key Nr** box.

9. This feature is currently NOT a function supported by the SAM. It is reserved for future versions.

Clicking the **<Get Key Entry>** box will **only return the key version** of key a, b and c packed in one byte for each key.

Remark: This command can be issued without valid (host) authentication.

4.4.3 Change KUC Entry

This command allows updating any Key Usage Counter (KUC) entry stored in the DESFireSAM.

The Limit, Key No of the Change Key Usage Counter (CKUC) and the version number of the CKUC can be changed selectively by checking the appropriate box and entering the new values.

Clicking the **<Change KUC Entry>** box will change the entry in the KUC.

Remark: Successful host authentication with the key specified in **KeyNoCKUC** of current KUC entry is required.

4.4.4 Get KUC Entry

The Get KUC Entry command allows retrieving the key usage counter entry specified in the Reference Number KUC box.

Clicking the **<Get KUC Entry>** box will return the Key No of the Change Key Usage Counter, its version, the Current Value and the Limit.

Remark: This command can be issued without valid (host) authentication.

4.4.5 Prepare For Change PICC

This command prepares the DESFireUI to be able to change the keys using the SAM. Both the current and the new key need to be present in the DESFireSAM prior to executing this command. The actual change of the keys can be done with the Change Key command in the DESFire Commands (see Section 3.4.5). The DESFireUI then uses the SAM ChangeKeyPICC command to generate the cryptogram that is sent to the DESFire to change one of its keys.

The method of key generation can be selected with radio buttons for:

- Involvement of Change Key key
- Setting of diversification for new key
- Status of diversification for current key

This command needs values for:

- KeyNo current key
- Key version current key
- KeyNo New key
- Key version New key

For key diversification the DESFire SAM uses the specified DES / 3DES key and the unique ID of the DESFire. This number can be entered in the **UID** field.

Clicking the **<Prepare for Change Key PICC>** box will prepare the DESFireUI to be able to change a key in the DESFire using the DESFire SAM.

4.4.6 Dump Session Key

This command can be used to retrieve the session key generated by the SAM.

This feature is necessary if the host should handle cryptographic operations like en-/decipher, instead of the SAM.

Clicking the **<Dump Session Key>** box will return the session key generated by the SAM and displays it in the transaction log window.

Remark: As this feature can be seen as a potential security risk if not used in the correct way, it can be en-/disabled using the configuration settings of every key entry.

4.5 Security Related Commands

This group contains the security related commands of the DESFire.

4.5.1 Authenticate Host

This command is used to run a mutual 3-pass authentication between the SAM and host system.

Remark: For details on the method used for session key generation, please refer to "Functional Specification" of DESFire PICC.

4.5.2 Select Application

This command is the equivalent of the **SelectApplication** command of the DESFire.

The DESFire AID can be entered in the **SAM AID** field.

Clicking the **<Select Application>** box will generate a list with a maximum of two keys per DESFire key number in the RAM of the DESFire SAM, from the key storage table. This allows the user to quickly address a key for this DF AID. For every DESFire key number up to 6 keys can be stored in this list (only the keys from two key entries in the key storage table will be stored with 3 key versions each). The key storage table is searched starting with key entry zero. If more than 6 key versions per DESFire AID and DESFIRE key number are found in key entries, only the first 6 versions will be stored in the RAM of the DESFireSAM.

4.5.3 Prepare For Authenticate PICC

This command prepares the DESFireUI to authenticate the DESFire using the SAM. The actual authentication can be done with the Authenticate command in the DESFire Commands (see Section 3.4.1).

There are two ways to specify the key number that will be used:

- If a **Select Application** command has been completed successfully preceding **Authenticate_PICC**, the same key number as used on DESFire can be send in the KeyNo parameter. Valid range for the number is 00h to 0Dh.
- If no **Select Application** command has been completed, the reference number of the key entry must be entered as parameter KeyNo.

Diversified Authentication requires the UID of the DESFire. If that box is checked, the UID can be entered in the **UID** text input field.

Clicking the **<Prepare for Authenticate PICC>** box will prepare the DESFireUI to perform the authentication with the DESFire using the SAM.

4.5.4 Load Init Vector

This command can be used to load an Init Vector to the 3DES coprocessor of the DESFire SAM. This is necessary if the **Keep DES IV** setting of the key entry is enabled and a special value for the Init Vector must be entered

The Init Vector can be entered in the **Init Vector** text input field.

Clicking the **<Load Init Vector>** box will load the Init Vector in the 3DES coprocessor.

4.6 General Commands

4.6.1 Get Version

The Get Version command returns manufacturing related data of the SAM.

Clicking the **<Get Version>** box will retrieve the manufacturing data and display it in the transaction window.

This command will also retrieve the unique ID of the DESFireSAM and automatically populate the entries where that unique ID is required.

Remark: This command can be issued without valid (host) authentication.

4.7 Setter and Getter methods

The SetInitVector and GetInitVector methods are used in the DESFire library for setting or getting the internal init vector for cryptographic operations stored in the library. This is necessary in case the SAM is configured for storing the init vector.

For example:

You activate the SAM and issue a host authentication (key is configured for keeping the init vector). Now the SAM keeps the init vector and the library has the correct init vector stored internally. If you now call the Encipher function, the SAM has afterwards a new init vector stored, but the library itself does not decipher the data and is therefore not able to create the correct init vector for the next operation. Only the application that uses and deciphers the data knows the init vector. If the next step is to change a key entry in the SAM, the init vector has to be set correctly so that the library is able to calculate the correct data block. If now the application wants to encipher a block that shall then be deciphered by the SAM, it has to call the GetInitVector function to retrieve the current init vector.

Remark: The methods are included in the DESFireUI because of their availability in the DESFire library. An ordinary user of the DESFireUI will most likely never use them.

4.7.1 Set Init Vector

This command allows storing an Init Vector in the coprocessor of the DESfireSAM.

The Init Vector can be entered in the **Init Vector** text input box or selected via the drop-down box.

Clicking the **<Set Init Vector>** box will store the Init Vector in the DESFireSAM reader library for applying it in the next cryptographic operation.

4.7.2 Get Init Vector

This command allows retrieving the Init Vector from the coprocessor of the DESfireSAM.

Clicking the **<Get Init Vector>** box will retrieve the Init Vector from the DESFireSAM reader library and display the result in the transaction log window.

5. Use Examples/Exercises

5.1 Change keys in DESFire

5.1.1 Change Master Key or Change Key

Step	Action
1	Put DESFire card on RD700 or RD701 reader
2	Start DESFireUI program
3	Unfold DESFire Commands
4	Select PCD Commands
	Click **<Interface Open>** box
5	Select T=CL Commands
	Click **<Activate Idle>** box
	Click **<RATS>** box
6	Unfold Security Commands
7	Select Authenticate
	Select **Key Number** zero
	Enter all zeroes for **Key** value[10].
	Click **<Authenticate>** box
8	Select Format PICC
	Click **<Format Picc>** box (to empty DESFire PICC)
9	Unfold PICC commands
10	Select Create Application
	Enter 111111h for **Application ID**
	Enter 14 for **Number of Keys**
	Check **Configuration Changeable**
	Check **Free create/delete without masterkey**
	Check **Free directory list access without masterkey**
	Check **Allow masterkey change**
	Enter 10 for **Change Key access rights**
	Click **<Create App>** box
11	Select Select Application
	Enter (or Select) 111111h for **Application Id**
	Click **<Select App>** box
12	Select Authenticate
	Select **Key Number** zero
	Enter all zeroes for **Key** value

10. If the DESFire PICC is not in virgin state, please enter the Key value of the masterkey

Step	Action
	Click **<Authenticate>** box
13	Select Change Key
	Select **Key Number** zero
	Enter FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFh for **Key** value
	Empty **Prev Key** field (make sure to remove all the spaces!)
	Click **<Change Key>** box
14	Select Authenticate
	Select **Key Number** zero
	Enter (or select) FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFh for **Key** value
	Click **<Authenticate>** box (and watch the transaction log windows for OK result to prove that the key was changed)
15	In T=CL Commands click **<Deselect>** box to deselect the DESFire
16	Exit DESFireUI program

5.1.2 Change ordinary key

Remark: This example assumes using the card that has been configured in Section 5.1.1

Step	Action
1	Put DESFire card on RD700 or RD701 reader
2	Start DESFireUI program
3	Unfold DESFire Commands
4	Select PCD Commands
	Click **<Interface Open>** box
5	Select T=CL Commands
	Click **<Activate Idle>** box
	Click **<RATS>** box
6	Unfold PICC commands
7	Select Select Application
	Enter (or Select) 111111h for **Application Id**
	Click **<Select App>** box
8	Unfold Security Commands
9	Select Authenticate
	Select **Key Number** 10 (remember, this was defined as the Change Key)
	Enter 00000000000000000000000000000000h for **Key** value
	Click **<Authenticate>** box
10	Select Change Key
	Select **Key Number** 1
	Enter 11111111111111111111111111111111h for **Key** value
	Enter 00000000000000000000000000000000h for **Prev Key** value
	Click **<Change Key>** box
11	Select Authenticate
	Select **Key Number** 1
	Enter 11111111111111111111111111111111h for **Key** value
	Click **<Authenticate>** box (and watch the transaction log windows for OK result)
12	In T=CL Commands click **<Deselect>** box to deselect the DESFire
13	Exit DESFireUI program

5.2 Command execution times for DESFire

5.2.1 Using standard baud rates

Step	Action
1	Put DESFire card on RD700 or RD701 reader
2	Start DESFireUI program
3	Unfold DESFire Commands
4	Select PCD Commands
	Click **<Interface Open>** box
	Check **Automatically retrieve command times**
5	Select T=CL Commands
	Click **<Activate Idle>** box
	Click **<RATS>** box
6	Unfold Security Commands
	Select Authenticate
	Select **Key Number** zero
	Enter all zeroes for **Key** value[11]
	Click **<Authenticate>** box
7	Select Format PICC
	Click **<Format Picc>** box (to empty DESFire PICC)
8	Unfold PICC commands
9	Select Create Application
	Enter 123456h for **Application Id**
	Enter 01 for **Number of Keys**
	Check **Configuration Changeable**
	Check **Free create/delete without masterkey**
	Check **Free directory list access without masterkey**
	Check **Allow masterkey change**
	Enter 14 for **Change Key access rights**
	Click **<Create App>** box
10	Select Select Application
	Enter (or Select) 123456h for **Application Id**
	Click **<Select App>** box
11	Unfold Application Commands
12	Select Create Data File
	Enter 11 for **File Id**
	Check **Plain communication**

11. If the DESFire PICC is not in virgin state, please enter the Key value of the masterkey

Step	Action
	Enter 14 for **Read Access**
	Enter 14 for **Write Access**
	Enter 14 for **Read/Write Access**
	Enter 14 for **Change Access Rights**
	Enter 3872 for **File Size**
	Click **<Create Data File>** box
13	Unfold File Commands
14	Select Data File Access
	Enter (or select) 11 for **File Id**
	Enter zero for **Length** (to read the entire file)
15	In lower left corner of window, click **<Reset Total Time>** box
16	In Data File Access click **<Read Data>** box
17	Read Total Execution Time in **Total Time** Window
	Remark: Repeat steps 15 and 17 a few times for consistent timings
18	In T=CL Commands click **<Deselect>** box to deselect the DESFire
19	Exit DESFireUI program

5.2.2 Using baud rates up to 424 kbit/s

Remark: This example assumes using the card that has been configured in Section 5.2.1

Step	Action
1	Start DESFireUI program
2	Put card on RD701 reader[12]
3	Unfold DESFire Commands
4	Select PCD Commands:
	Click **<Interface Open>** box
	Check **Automatically retrieve command times**
	Click **<Enable High Baud rates>** box
5	Select T=CL Commands
	Click **<Activate Idle>** box
	Click **<RATS>** box
	Select 2 for **DSI** (424 kbit/s)[13]
	Select 2 for **DRI** (424 kbit/s)
	Click **<PPS>** box
6	Unfold PICC commands
7	Select Select Application
	Enter (or Select) 123456h for **Application Id**
	Click **<Select App>** box
8	Unfold File Commands
9	Select Data File Access
	Enter (or select) 11 for **File Id**
	Enter zero for **Length** (to read entire file)
10	In lower left corner of window, click **<Reset Total Time>** box
11	In Data File Access click **<Read Data>** box
12	Read Total Execution Time with higher baud rates in **Total Time** Window
	Remark: Repeat steps 10 and 12 a few times for consistent timings
13	In T=CL Commands click **<Deselect>** box to deselect the DESFire
14	Exit DESFireUI program

12. This DESFire data rate example can only be executed with the RD701 reader because that is able to support higher baud rates.
13. Coding for DSI & DRI: 0 = 106 kbit/s; 1 = 212 kbit/s; 2 = 424 kbit/s; 3 = 848 kbit/s

5.3 Use of Key Usage Counters of DESFireSAM

Step	Action
1	Put DESFireSAM card in smartcard reader with PC/SC interface
2	Start DESFireUI program
3	Unfold DESFireSAM Commands
4	Select SAM Activation and Click **<Activate SAM>** box (**Select DESFire SAM** window will indicate that SAM has been selected)
	Click **<OK>** box to continue[14]
5	Unfold Key Handling Commands
6	Select Get KUC Entry
	Enter (or select) 0Fh for **Reference number KUC**
7	Click **<Get KUC Entry>** box and watch of current value of **Key Usage Counter**
8	Unfold Security Related Commands
9	Select Authenticate Host
	Enter (or select) 00h for **KeyNo** and 00h for **KeyV**
	Check **Generate Session Key**
	Enter (or select) all zeroes for **Secret Key**[15]
	Click **<Authenticate Host>** box
10	Select Change Key Entry
	Enter (or select) 0Fh for **RefNoKUC**
	Check **Update Reference number of KUC**
	Enter (or select) 00h for **Nr. of Key to change**
	Click **<Change Key Entry>** box
11	Select Authenticate Host
	Enter (or select) 00h for **KeyNo** and 00h for **KeyV**
	Check **Generate Session Key**
	Enter (or select) all zeroes for **Secret Key** for **Secret Key** [15]
	Click **<Authenticate Host>** box
12	Select Get KUC Entry
	Enter (or select) 0Fh for **Reference number KUC**
	Click **<Get KUC Entry>** box and watch current value of **Key Usage Counter**
	Remark: Repeat steps 11 and 12 a few times to see the increase of the KUC
13	In SAM Activation click **<Deactivate SAM>** box
14	Exit DESFireUI program

14. In some systems it may be necessary to physically remove the SAM card and re-insert it before this the SAM can be recognized in the reader
15. If the DESFireSAM is not in virgin state, please enter the Key value of KeyNo 0x00

5.4 Key change in DESFireSAM

Step	Action
1	Put DESFireSAM card in smartcard reader with PC/SC interface
2	Start DESFireUI program
3	Unfold DESFireSAM Commands
4	Select SAM Activation and Click **<Activate SAM>** box (**Select DESFire SAM** window will indicate that SAM has been selected)
	Click **<OK>** box to continue[16]
5	Unfold Security Related Commands
6	Select Authenticate Host
	Enter (or select) 00h for **KeyNo** and 00h for **KeyV**
	Check **Generate Session Key**
	Enter (or select) all zeroes for **Secret Key**[17]
	Click **<Authenticate Host>** box
7	Unfold Key Handling Commands
	Select **Change Key Entry**
	Enter 11111111111111111111111111111111h for **Key A**
	Enter 22222222222222222222222222222222h for **Key B**
	Check **Update Key Version A**
	Check **Update Key Version B**
	Enter (or select) 01h for **Nr. of Key to change**
	Click **<Change Key Entry>** box
8	Select Get Key Entry
	Select **Key Nr.** 01h and Click **<Get Key Entry>** box
9	Select Authenticate Host
	Enter (or select) 01h for **KeyNo** and FFh for **KeyV**
	Check **Generate Session Key**
	Enter 11111111111111111111111111111111h for **Secret Key**
	Click **<Authenticate Host>** box (and watch the transaction log windows for OK result)
	Enter (or select) 01h for **KeyNo** and 00h for **KeyV**
	Enter 22222222222222222222222222222222h for **Secret Key**
	Click **<Authenticate Host>** box (and watch the transaction log window for OK result)
10	Select SAM Activation and Click **<Deactivate SAM>** box
11	Exit DESFireUI program

16. In some systems it may be necessary to physically remove the SAM card and re-insert it before this the SAM can be recognized in the reader
17. If the DESFireSAM is not in virgin state, please enter the Key value of KeyNo 0x00

5.5 DESFire authentication using DESFireSAM

Remark: This example assumes using the DESFire card that has been configured in Section 5.1.1 and Section 5.1.2 and the DESFire SAM that has been configured in Section 5.4

Step	Action
1	Put DESFireSAM card in smartcard reader with PC/SC interface
2	Put DESFire card on RD700 or RD701 reader
3	Start DESFireUI program
4	Unfold DESFire Commands
5	Select PCD Commands and Click **<Interface Open>** box
6	Select T=CL Commands
	Click **<Activate Idle>** box
	Click **<RATS>** box
7	Unfold PICC commands
8	Select Select Application
	Enter (or Select) 111111h for **Application Id**
	Click **<Select App>** box
9	Unfold DESFireSAM Commands
10	Select SAM Activation
	Click **<Activate SAM>** box (**Select DESFire SAM** window will indicate that SAM has been selected)
	Click **<OK>** box to continue[18]
11	Unfold Security Related Commands
12	Select Prepare for Authenticate PICC
	Enter (or select) 01h for **KeyNo** and FFh for **KeyV**
	Make sure that **Non Diversified Authentication** and **Select by Key Entry number** are checked
13	Click **<Prepare for Authenticate PICC>** box
14	Unfold Security Commands
15	Select Authenticate
	Enter (or select) 01 for **Key Number** remark that no key can be entered, since the authentication will be performed through the SAM)
	Click **<Authenticate PICC>** box

18. In some systems it may be necessary to physically remove the SAM card and re-insert it before this the SAM can be recognized in the reader

Step	Action
16	In T=CL Commands click **<Deselect>** box to deselect the DESFire
17	In SAM Activation click **<Deactivate SAM>** box
18	Exit DESFireUI program

5.6 DESFire key change using DESFireSAM

Remark: This example assumes using the DESFire card that has been configured in Section 5.1.1 and Section 5.1.2 and the DESFire SAM that has been configured in Section 5.4

Step	Action
1	Put DESFireSAM card in smartcard reader with PC/SC interface
2	Put DESFire card on RD700 or RD701 reader
3	Start DESFireUI program
4	Unfold DESFire Commands
5	Select PCD Commands
	Click **<Interface Open>** box
6	Select T=CL Commands
	Click **<Activate Idle>** box
	Click **<RATS>** box
7	Unfold PICC commands
8	Select Select Application
	Enter (or Select) 111111h for **Application Id**
	Click **<Select App>** box
9	Unfold DESFireSAM Commands
10	Select SAM Activation
	Click **<Activate SAM>** box (**Select DESFire SAM** window will indicate that SAM has been selected)
	Click **<OK>** box to continue[19]
11	Unfold Security Related Commands
12	Select Authenticate Host
	Enter (or select) 00h for **KeyNo** and 00h for **KeyV**
	Check **Generate Session Key**
	Enter (or select) all zeroes for **Secret Key**[20]
	click **<Authenticate Host>** box
13	Unfold Key Handling Commands
14	Select Change Key Entry
	Enter 111111h for **DF AID** and 01h for **DF KeyNo**

19. In some systems it may be necessary to physically remove the SAM card and re-insert it before this the SAM can be recognized in the reader
20. If the DESFireSAM is not in virgin state, please enter the Key value of KeyNo 0x00

Step	Action
	Enter 11111111111111111111111111111111h for **Key A**
	Check **Update DF key number and DF AID**
	Check **Update Key Version A**
	Enter (or select) 01h for **Nr. of Key to change**
	Click **<Change Key Entry>** box
	Enter aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaah for **Key A** [21]
	Enter (or select) 02h for **Nr. of Key to change**
	Click **<Change Key Entry>** box
15	Select Prepare for Authenticate PICC
	Enter (or select) 00h for **KeyNo** and 00h for **KeyV**
	Make sure that **Non Diversified Authentication** and **Select by Key Entry number** are checked
	Click **<Prepare for Authenticate PICC>** box
16	Select Authenticate in DESFire Security Commands
	Enter (or select) 10 for **Key Number** (note that no key can be entered, since the authentication will be performed through the SAM)
	Click **<Authenticate>** box
17	Select Prepare for Change Key PICC
	Enter (or select) 01h for **KeyNo Old** and FFh for **KeyV Old**
	Enter (or select) 02h for **KeyNo New** and 00h for **KeyV New**
	Make sure that **Don't Change Master Key**, **Don't Diversify New Key** and **Current key is Not Diversified** are checked
18	Click **<Prepare for Change Key PICC>** box
19	Select Change Key in DESFire Security Commands
	Enter (or select) 01 for **Key Number**
	Click **<Change Key>** box
20	In SAM Activation click **<Deactivate SAM>** box
21	Select Authenticate in DESFire Commands
	Select **Key Number** 01 (remember, this was defined as the Change Key)
	Enter aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaah for **Key** value
	Click **<Authenticate>** box
22	In T=CL Commands click **<Deselect>** box to deselect the DESFire
23	Exit DESFireUI program

21. Since the program does not allow you to enter 16 capital As, you need to enter them in lower case

6. Abbreviations

Table 2: Abbreviations

Acronym	Description
AID	Application ID
APDU	Application Protocol Data Unit
ATS	Answer To Select
CID	Card IDentifier
CBC	Cipher-Block Chain
CEK	Change Entry Key
DES	Data Encryption Standard
DF	DESFire
DRI	Divisor Receive Integer (PCD to PICC)
DSI	Divisor Send Integer (PICC to PCD)
FID	File ID
FSCI	Frame Size for proximity Card Integer
FSDI	Frame Size for proximity coupling Device Integer
FWI	Frame Waiting time Integer
FWT	Frame Waiting Time
INF	INformation Field
KUC	Key Usage Counter
MAC	Message Authentication Code
NAD	Node ADdress
PCB	Protocol Control Byte
PCD	Proximity Coupling Device (reader/writer unit)
PICC	Proximity Integrated Circuit Card
PPS	Protocol and Parameter Selection
RATS	Request for Answer To Select
REQA	REQuest Command, Type A
RFU	Reserved for Future Use
SAK	Select AcKnowledge
SAM	Secure Application Module
UID	Unique IDentification number
WTX	Waiting Time eXtension

7. References

[1] **Data sheet —** MF3 IC D40 mifare DESFire; Contactless Multi-Application IC with DES and 3DES Security

[2] **Application Note —** MF3 IC D40 mifare DESFire; Features and Hints

[3] **Functional specification —** DESFire SAM; Reader Module for MF3 IC D40

[4] **Functional specification —** DESFire SAM MAC; MACing Reader Module for MF3 IC D40

8. Disclaimers

Life support — These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Philips Semiconductors customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Philips Semiconductors for any damages resulting from such application.

Right to make changes — Philips Semiconductors reserves the right to make changes in the products - including circuits, standard cells, and/or software - described or contained herein in order to improve design and/or performance. When the product is in full production (status 'Production'), relevant changes will be communicated via a Customer Product/Process Change Notification (CPCN). Philips Semiconductors assumes no responsibility or liability for the use of any of these products, conveys no licence or title under any patent, copyright, or mask work right to these products, and makes no representations or warranties that these products are free from patent, copyright, or mask work right infringement, unless otherwise specified.

Application information — Applications that are described herein for any of these products are for illustrative purposes only. Philips Semiconductors make no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

9. Trademarks

Mifare — is a trademark of Koninklijke Philips Electronics N.V.

DESFire — is a trademark of Koninklijke Philips Electronics N.V.

10. Contents

Date of release:27 May 2005
BLID Document number: M111010

Published in Austria